THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

EUDOICE HENDRIX, on behalf of himself and all others similarly situated, Plaintiff, v. GLOBAL ATLANTIC FINANCIAL COMPANY, ACCORDIA LIFE AND ANNUITY COMPANY, COMMONWEALTH ANNUITY AND LIFE INSURANCE COMPANY, FIRST ALLMERICA FINANCIAL LIFE INSURANCE COMPANY, and FORETHOUGHT LIFE INSURANCE COMPANY, Defendants.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Eudoice Hendrix ("Plaintiff") brings this Class Action Complaint against Global Atlantic Financial Company ("GAFC"), Accordia Life and Annuity Company ("Accordia"), Commonwealth Annuity and Life Insurance Company ("Commonwealth"), First Allmerica Financial Life Insurance Company ("First Allmerica"), and Forethought Life Insurance Company ("Forethought") (collectively, "Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly

secure and safeguard personal identifiable information ("PII")[1] of more than 130,000 individuals, including, but not limited to, names, policy numbers, Social Security numbers, dates of birth, gender, and address data.

2. Defendants sell life insurance and annuities.

3. Defendants' headquarters are in New York, NY.

4. Defendant GAFC has a 100% ownership interest in Commonwealth, which in turn has a 100% ownership interest in each of Accordia, First Allmerica, and Forethought.

5. Defendants' Privacy Statement states as follows:

> **Protecting Personal Information**
>
> To protect your information from unauthorized access and use, we have adopted security measures that comply with applicable law, and are reasonably designed to protect the availability, confidentiality, and integrity of your personal information. Although we do our best to protect your personal information, we cannot guarantee the security of your personal information transmitted to our website. Any electronic transmission of personal information (e.g., over the Internet) is at your own risk, and Global Atlantic is not responsible for circumvention of any privacy settings or security measures contained on its website. TO THE EXTENT PERMITTED BY LAW, WE SHALL NOT BE LIABLE OR OTHERWISE RESPONSIBLE FOR ANY DATA INCIDENT OR EVENT THAT MAY COMPROMISE THE CONFIDENTIALITY, INTEGRITY, OR SECURITY OF YOUR PERSONAL INFORMATION CAUSED BY A THIRD PARTY. The safety and security of your personal information also depends on you. Where we have given you (or where you have chosen) a user name and password to access our websites or online accounts, you are responsible for maintaining the security and confidentiality of those credentials. You must immediately contact us if you know, or have reason to suspect, that your user name or password to our website or online account has been compromised or otherwise subject to unauthorized access, use, or disclosure. You acknowledge and agree that we may contact you via email or other electronic

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

communications in the event we are legally required to notify you of a data security incident or event related to your personal information.

Information Stored in the United States

Global Atlantic is headquartered in the United States, and the information (including personal information) that we collect is most often stored, and retained, in the United States. If you are located outside of the United States, please be aware that information you submit will be transferred to the United States, and that the United States may not provide the same level of protections as the laws in your country of residence. By continuing to provide us such information you hereby consent to this transfer.

Retention of Personal Information

Global Atlantic retains your personal information for the time period reasonably necessary to satisfy the purpose it was collected for, or as long as necessary to comply with legal obligations, or for the establishment, exercise, or defense of a legal claim. Generally, we retain your personal information for the duration needed to complete, or facilitate, a contract, agreement, or engagement, and for a reasonable amount of time thereafter in accordance with our legitimate business needs and functions, or in compliance with applicable laws.[2]

6. Defendants' 2022 Corporate Responsibility Report states as follows:

Data Privacy & Security

Cyber Risk

Global Atlantic utilizes wide-ranging security measures to preserve the confidentiality, integrity and availability of information entrusted to us by all parties that conduct business with us. These measures include written policies, controls, standards and processes, protection and detection systems, awareness and training, and security risk assessments of both our Information Security Program and third parties.

Our Information Security Program is premised upon the National Institute of Standards and Technology Cybersecurity Framework, NIST 800 Series publications and industry best practices. Our Chief Information Security Officer (CISO) is accountable for maintaining

[2] Exhibit 1.

> the Information Security Program and all cybersecurity-related activities within Global Atlantic. Our CISO works in partnership with our Chief Privacy Officer in maintaining privacy-related safeguards and oversight within Global Atlantic. Our CISO provides reporting on the state of the cybersecurity program, any matters that have been identified, and plans to remediate such matters to our Board of Directors and the Risk Committee on a regular basis.
>
> **Key Components of the Information Security Program**
>
> - Maintain information security policies, controls and standards.
> - Present the state of our Information Security Program to our Management Committee and Board of Directors on a regular basis and in compliance with cybersecurity and other legal and regulatory requirements.
> - Conduct ongoing risk assessments, including third-party risk assessments, penetration testing and vulnerability scanning.
> - Partner with teams across Global Atlantic to enhance technical safeguards and protect our information assets based on risk.
> - Maintain our information security incident response plan and coordinate with the relevant functional area to test the plan (at least annually) and adjust the plan, if necessary.
> - Provide continuous cybersecurity awareness training to all employees, including through our Annual Data Privacy and Cybersecurity Awareness Month.

7. Prior to and through May 30, 2023, Defendants obtained the PII of Plaintiff and Class Members, including by collecting it directly from Plaintiff and Class Members.

8. Prior to and through May 30, 2023, Defendants shared the PII of Plaintiff and Class Members, unencrypted, with their third-party administrator to perform "death matching" services to determine whether policyholders are alive.

9. Prior to and through May 30, 2023, Defendants' third-party administrators shared the PII of Plaintiff and Class Members, unencrypted, with Pension Benefits Information, LLC

("PBI"), ostensibly to perform regulatory compliance and operational support services.

10. On or before June 2, 2023, Defendants learned of a data breach involving the "MoveIT" secure file transfer application, which PBI used (the "Data Breach").

11. Defendants determined that, during the Data Breach, an unknown actor acquired the unencrypted PII of Plaintiff and Class Members.

12. On or around August 11, 2023, Defendants began notifying various states Attorneys General of the Data Breach. Defendants' report filed with the Attorney General of Texas states Defendants' address is 30 Hudson Yards, New York, New York, 10001. This is also the principal address of GAFC.

13. On or around August 11, 2023, Defendants began notifying Plaintiff and Class Members of the Data Breach.

14. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendants admit that the unencrypted PII that was accessed and/or acquired by an unauthorized actor included names, policy numbers, Social Security numbers, dates of birth, gender, and address data.

15. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive information.

16. The PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members, including the failure

to encrypt the PII and the failure to include that entities with which Defendants shared the PII maintained it in encrypted form.

17. As a result of the Data Breach, Plaintiff and Class Members are, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

18. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiff and Class Members; and (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices. Defendants' conduct amounts to negligence and violates federal and state statutes.

19. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

20. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable,

required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

21. Plaintiff is a citizen of Arkansas residing in London, Arkansas.

22. Defendant GAFC is a Delaware corporation with a principal place of business in New York, New York.

23. Defendant Accordia is an Iowa corporation with a principal place of business in Des Moines, Iowa.

24. Defendant Commonwealth is a Massachusetts corporation with a principal place of business in Brighton, Massachusetts.

25. Defendant First Allmerica is a Massachusetts corporation with a principal place of business in Brighton, Massachusetts.

26. Defendant Forethought is an Indiana corporation with a principal place of business in Indianapolis, Indiana.

27. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

28. All of Plaintiff's claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

29. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiff, is a citizen of a state different from Defendants to establish minimal diversity.

30. Defendant GAFC is a citizen of Delaware and New York because it is a corporation formed under Delaware law with its principal place of business in New York, New York.

31. Defendant Accordia is a citizen of Iowa because it is a corporation formed under Iowa law with its principal place of business in Des Moines, Iowa.

32. Defendant Commonwealth is a citizen of Massachusetts because it is a corporation formed under Massachusetts law with its principal place of business in Brighton, Massachusetts.

33. Defendant First Allmerica is a citizen of Massachusetts because it is a corporation formed under Massachusetts law with its principal place of business in Brighton, Massachusetts.

34. Defendant Forethought is a citizen of Indiana because it is a corporation formed under Indiana law with its principal place of business in Indianapolis, Indiana.

35. The Southern District of New York has personal jurisdiction over Defendants because they conduct substantial business in New York and this District, collected and/or stored the PII of Plaintiff and Class Members in this District, and formed and implemented policies and procedures related to safeguarding Plaintiff's and Class Members' PII in this District.

36. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants operate in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, including Defendants collecting and/or storing the PII of Plaintiff

and Class Members and Defendants' formation and implementation of policies and procedures related to safeguarding Plaintiff's and Class Members' PII.

IV. FACTUAL ALLEGATIONS

Background

37. Defendants collected the PII of Plaintiff and Class Members and shared it, unencrypted, with their third-party administrator, which in turn shared it with PBI.

38. Plaintiff and Class Members relied on these sophisticated Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

39. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

The Data Breach

40. On or about August 11, 2023, Defendants sent Plaintiff and Class Members a *Notice of Cybersecurity Incident* and submitted sample notices to various states' Attorneys General. Defendants informed Plaintiff and other Class Members that:

> At Global Atlantic, we do our best to protect your personal information and ensure our business partners do the same. Despite these efforts, we have been informed by Pension Benefits Information LLC ("PBI") that they recently experienced a cybersecurity incident involving the MOVEit file transfer application, and that the incident has impacted our policyholder data. PBI is a third-party vendor that Global Atlantic uses to satisfy applicable regulatory obligations to identify the deaths of insured persons, which can impact premium payment obligations and benefit eligibility. PBI is one of hundreds of companies across a variety of industries that have been impacted by the MOVEit incident.
>
> **[Is_Policy_Active], we believe that the following types of**

> **personal identifiable information related to you were impacted: Name, [Data_Elements].**
>
> Please note that Global Atlantic's environment was not compromised as a part of this incident. It is still safe to interact with our corporate systems and our website.[3]

41. Plaintiff's *Notice of Cybersecurity Incident* states that his name, Social Security number, date of birth, and policy number were impacted in the Data Breach.

42. Defendants admitted in the *Notice of Cybersecurity Incident* and the sample notices and reports they sent to the states' Attorneys General that an unauthorized actor may have acquired sensitive information about Plaintiff and Class Members, including names, policy numbers, Social Security numbers, dates of birth, gender, and address data.

43. In response to the Data Breach, Defendants claim that, because the Data Breach did not occur on their systems, they "did not conduct an internal review of [their] controls in response to this incident" and "[are] not taking efforts to recover the data, and [are] unaware of any efforts by PBI to recover the data."[4]

44. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

45. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

---

[3] Exhibit 2 (Defendants' letter and sample notice to Iowa Consumer Protection Division).
[4] *Id.*

46. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

47. Prior to the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack on third parties with which Defendants shared the PII.

48. Prior to the Data Breach, Defendants knew or should have known that they should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack on third parties with which Defendants shared the PII.

49. Prior to the Data Breach, Defendants knew or should have known that they should have ensured that third parties with which they shared the PII encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Defendants Acquire, Collect, and Store the PII of Plaintiff and Class Members.

50. Defendants acquired, collected, and stored the PII of Plaintiff and Class Members.

51. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

52. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

53. Defendants could have prevented this Data Breach by properly encrypting the PII of Plaintiff and Class Members and ensuring that third parties with which Defendants shared the PII maintained it in encrypted form.

54. Defendants' negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

55. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

56. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[5] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[6]

57. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

58. The PII of individuals remains of high value to criminals, as evidenced by the prices

[5] 17 C.F.R. § 248.201 (2013).

[6] *Id.*

they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[7] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[8] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[9]

59. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

60. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[10]

61. Among other forms of fraud, identity thieves may obtain driver's licenses,

---

[7] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Feb. 24, 2023).

[8] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Feb. 24, 2023).

[9] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Feb. 24, 2023

[10] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Feb. 24, 2023).

government benefits, medical services, and housing or even give false information to police.

62. The fraudulent activity resulting from the Data Breach may not come to light for years.

63. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

64. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur from the breach of a data security system of a third party with which Defendants shared the PII, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

65. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring the dark web and other potential indicators of misuse of their information, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

66. Defendants were, or should have been, fully aware of the unique type and the significant volume of data contained in the PII they shared with their third-party administrator and PBI, amounting to thousands of individuals' detailed, personal information and, thus, the

[11] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Feb. 24, 2023).

significant number of individuals who would be harmed by the exposure of the unencrypted data.

67. To date, Defendants have offered Plaintiff and Class Members two years of identity theft detection through Experian. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

68. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff's Experience

69. Plaintiff obtained an annuity from Forethought prior to the Data Breach and received Defendants' *Notice of Cybersecurity Incident*, dated August 11, 2023, on or about that date. Plaintiff's notice stated that his name, Social Security number, date of birth, and policy number were impacted.

70. As a result of the Data Breach, Plaintiff's sensitive information was accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff will have to worry about when and how his sensitive information may be shared or used to his detriment.

71. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Security Incident* and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

72. Additionally, Plaintiff is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

73. Plaintiff stores any documents containing his sensitive PII in a safe and secure

location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

74. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

75. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

76. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

77. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

78. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals whose PII was accessed and/or acquired in the data incident that is the subject of the Notice of Cybersecurity Incident that Defendants sent to Plaintiff and Class Members on or around August 11, 2023 (the "Nationwide Class").

79. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Florence asserts claims on behalf of a separate statewide subclass, defined as follows:

> All individuals who obtained insurance or an annuity from Forethought and whose PII was accessed and/or acquired in the data incident that is the subject of the Notice of Cybersecurity Incident that Defendants sent to Plaintiff and Class Members on or around August 11, 2023 (the "Forethought Subclass") (collectively, with

the Nationwide Class, "the Classes").

80. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

81. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

82. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendants reported to the Texas Attorney General that 87,638 Texas residents were impacted in the Data Breach, reported to the Massachusetts Attorney General that 15,560 Massachusetts residents were impacted in the Data Breach, reported to the South Carolina Attorney General that 14,913 South Carolina residents were impacted in the Data Breach, reported to the Iowa Attorney General that 10,634 Iowa residents were impacted in the Data Breach, reported to the Delaware Attorney General that 5,732 Delaware residents were impacted in the Data Breach, and the Classes are apparently identifiable within Defendants' records.

83. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendants had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiff and Class Members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the

imminent and currently ongoing harm faced as a result of the Data Breach.

84. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

85. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

86. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

87. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary

duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

88. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

89. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

90. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

91. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper

notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

92. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

93. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information

compromised in the Data Breach;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

94. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

95. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

96. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

97. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII of Plaintiff and the Nationwide Class in Defendants' possession was adequately secured and protected.

98. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Nationwide Class.

99. Defendants' duty to use reasonable security measures arose as a result of the special

relationship that existed between Defendants and Plaintiff and the Nationwide Class. That special relationship arose because Defendants acquired Plaintiff's and the Nationwide Class's confidential PII in the course of their business practices.

100. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Nationwide Class.

101. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

102. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII, the necessity for encrypting PII shared with third parties, and the necessity for ensuring such third parties maintained the PII in encrypted form.

103. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendants.

104. Plaintiff and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

105. Defendants were in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

106. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiff and the Nationwide Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

107. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Nationwide Class.

108. Defendants have admitted that the PII of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

109. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Nationwide Class during the time the PII was within Defendants' possession or control.

110. Defendants improperly and inadequately safeguarded the PII of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

111. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Nationwide Class in the face of increased risk of theft.

112. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

113. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

114. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Nationwide Class would not have been compromised.

115. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

116. As a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect

the PII of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

117. As a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

118. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

119. As a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Forethought Subclass)

120. Plaintiff and the Forethought Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

121. Defendants' Privacy Statement states "[t]o protect your information from unauthorized access and use, we have adopted security measures that comply with applicable law, and are reasonably designed to protect the availability, confidentiality, and integrity of your personal information.

122. Defendants' 2022 Corporate Responsibility Report states they "utilize[] wide-ranging security measures to preserve the confidentiality, integrity and availability of information entrusted to us by all parties that conduct business with us. These measures include written policies, controls, standards and processes, protection and detection systems, awareness and training, and security risk assessments of both our Information Security Program and third parties."

123. In obtaining life insurance from Forethought, Plaintiff and the Forethought Subclass provided and entrusted their PII to Forethought.

124. Forethought required Plaintiff and the Forethought Subclass to provide and entrust their PII as condition of obtaining life insurance from Forethought.

125. As a condition of obtaining life insurance from Forethought, Plaintiff and the Forethought Subclass provided and entrusted their PII. In so doing, Plaintiff and the Forethought Subclass entered into implied contracts with Forethought by which Forethought agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiff and the Forethought Subclass if their PII had been compromised or stolen.

126. Plaintiff and the Forethought Subclass fully performed their obligations under the implied contracts with Forethought.

127. Forethought breached the implied contracts it made with Plaintiff and the Forethought Subclass by failing to adopt security measures that are reasonably designed to protect the availability, confidentiality, and integrity of personal information and failing to utilize wide-ranging security measures to preserve the confidentiality, integrity and availability of information entrusted to it by all parties that conduct business with it, including security risk assessments of third parties.

128. As a direct and proximate result of Forethought's above-described breach of implied contract, Plaintiff and the Forethought Subclass have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

129. As a direct and proximate result of Forethought's above-described breach of implied contract, Plaintiff and the Forethought Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT III
Violations of the New York General Business Law § 349
(On Behalf of Plaintiff and the Nationwide Class)

130. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 93.

131. Defendants' Privacy Statement states "[t]o protect your information from unauthorized access and use, we have adopted security measures that comply with applicable law, and are reasonably designed to protect the availability, confidentiality, and integrity of your personal information.

132. Defendants' 2022 Corporate Responsibility Report states they "utilize[] wide-ranging security measures to preserve the confidentiality, integrity and availability of information

entrusted to us by all parties that conduct business with us. These measures include written policies, controls, standards and processes, protection and detection systems, awareness and training, and security risk assessments of both our Information Security Program and third parties."

133. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. misrepresenting that they adopted security measures that are reasonably designed to protect the availability, confidentiality, and integrity of personal information; and

b. misrepresenting that they utilized wide-ranging security measures to preserve the confidentiality, integrity and availability of information entrusted to us by all parties that conduct business with us, including security risk assessments of third parties.

134. Defendants knew or should have known that their data security practices were inadequate to safeguard the PII that Plaintiff and the Nationwide Class entrusted to Defendants, and that risk of a data breach or theft was highly likely.

135. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

136. Defendants' failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and the Nationwide Class) regarding the protection of their PII.

137. The representations upon which consumers (including Plaintiff and the Nationwide Class) relied were material representations (*e.g.*, as to Defendants' adequate protection of PII), and

consumers (including Plaintiff and the Nationwide Class) relied on those representations to their detriment.

138. Defendants' conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiff and the Nationwide Class have been harmed, in that their PII was exposed to an unauthorized individual, which resulted in profound vulnerability to their personal information and other financial accounts.

139. As a direct and proximate result of Defendant'' unconscionable, unfair, and deceptive acts and omissions, the PII of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, which has caused and will continue to cause damage to Plaintiff and the Nationwide Class.

140. Plaintiff and the Nationwide Class seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

COUNT IV
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Nationwide Class)

141. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 81.

142. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

143. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and the Nationwide Class's PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and the Nationwide Class from further data breaches that compromise their PII. Plaintiff alleges that Defendants' data security measures remain inadequate. Defendants publicly deny these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendants have undertaken in response to the Data Breach.

144. Plaintiff and the Nationwide Class have an ongoing, actionable dispute arising out of Defendants' inadequate security measures, including (i) Defendants' failure to encrypt Plaintiff's and the Nationwide Class's PII, including Social Security numbers and (ii) Defendants' failure to ensured that third parties with which Defendants shared the PII stored it in encrypted form.

145. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure the PII of Plaintiff and the Nationwide Class;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendants' ongoing breaches of their legal duty continue to cause Plaintiff harm.

146. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry and

government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendants to:

a. audit, test, and train their data security personnel regarding any new or modified procedures and;

b. implement an education and training program for appropriate employees regarding cybersecurity.

147. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at one of the third parties with which Defendants share PII. The risk of another such breach is real, immediate, and substantial. If another such breach occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

148. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

149. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiff and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment

against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the Forethought Subclass and appointing Plaintiff and his Counsel to represent such Classes;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. requiring Defendants to establish an information security training program that

includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

vi. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

vii. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: September 12, 2023

Respectfully Submitted,

/s/ Jonathan M. Sedgh
Jonathan M. Sedgh

MORGAN & MORGAN
850 3rd Ave, Suite 402
Brooklyn, NY 11232
Phone: (212) 738-6839
Fax: (813) 222-2439
Email:jsedgh@forthepeople.com

Patrick A. Barthle*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
pbarthle@ForThePeople.com

Ryan D. Maxey*
MAXEY LAW FIRM, P.A.
107 N. 11th St. #402
Tampa, Florida 33602
(813) 448-1125
ryan@maxeyfirm.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice applications pending*